

Detection of Sybil attack using Clone Detection Mechanism in Wireless Sensor Networks

Manpreet Kaur^a, Anil Sagar^b, Baljinder Singh^c

^a Research Scholar, Beant College of Engineering and Technology, Gurdaspur, Punjab, India

^b Beant College of Engineering and Technology, Gurdaspur, Punjab, India

^c Beant College of Engineering and Technology, Gurdaspur, Punjab, India

Abstract: Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on. To detect and eliminate this type of attack, different detection techniques have been designed based on both static and mobile WSNs. Further, in this research work, firstly a node which wants to send data will fake broadcast which has to be replied by other nodes. Then, a node which is cloned will reply along with the reply of original node. These two will have same identities as ID for cloned node will be same as its original node. Thus, the cloned node with the original node will be banned for further transmissions. When, in future the node with same identity tries to enter, it will be blacklisted and hence could not enter in a network communication. Further performance is compared using 4 performance metrics.

Introduction

WSN is formed by many tiny, cheap low memory nodes and less energy, and process capability. In Such specific variety of WSNs, many issues arise to find out every node. Current advancements in wireless transmissions have facilitated to roll-out the cheap, less energy and versatile sensors that are tiny in size and transmit in a miniature distance. Inexpensive and good sensors are associated with the help of wireless channels and positioned in large amount. Moreover, the sensors which are associated or networked use a wide range of applications between the defense area, creating novel potential for intelligence and police work and numerous military science fields. Self-relocation capabilities are often an extremely fascinating sign of wireless device networks. The examples of environmental based applications are water quality checking and agriculture; the measuring data are not at all meaningful. Moreover, location estimation might alter several applications as an example of Intrusion Recognition, Stock Organization, Traffic Monitoring, Health Examination, intelligence and police work.

With all the development inside the reduction and incorporation of the finding and transmission technologies, the system of high level wireless mechanisms uses a considerable amount of economic sensors and low energy consumption previously realized. Within a wireless device system, the nodes of the powered devices are scattered in a physical space. Each device within the sensor network collects information, for example, detection of vibrations, temperature, radiation and various environmental factors.

2. Related Work

P. Dewal et. al. [1] Proposed that the special network based on the WSNs should be a small sensor network node installed in a specific area. They are inclined to advertise due to distributed behavior and implementation in distant areas. The black hole attack is a type of denial of service attack in which the attacker attracts all packets from the node and the packet is not forwarded. This document describes the cluster-based sensor network with two stacking heads in each cluster used for detection and prevention of black holes

S. Ali et. al. [2] Said that the WSNs is the combination of small devices called sensor nodes, gateways and software. These nodes use a wireless transmission medium and are able to detect and transmit data to other nodes. In general, WSN is composed of two types of nodes, namely generic nodes and gateway nodes. Generic nodes that are able to detect while gateway nodes are used to route such information. The IoT is now extended to IoET (Internet of Everything) to cover all existing electronic devices, such as body sensor networks, VANET, smart grid stations, smart phones, PDAs, autonomous cars, refrigerators and smart roasters able to communicate and sharing information using existing network technologies The sensor nodes in WSN have a very limited transmission range, as well as limited processing speed, memory capacity and low battery.

R.K Dwivedi et. al. [3] Said that the WSNs is a collection of different sensor nodes. These sensor nodes collect data from the environment and send it to their destination by following an appropriate path. A sensor network has several applications to monitor physical phenomena in military, agricultural and medical applications where it can be used to improve human life in many ways. There are many problems in WSN such as safety, energy efficiency and QoS, etc. requiring attention to today's investigations. There are several security attacks that affect the data dissemination process. These security attacks originate at different levels of the Internet model, which hinders network security. In this paper, a comparative study of some methods of detection and prevention of wormhole attack is presented. In the document the various models of wormhole attack and different wormhole attack nodes are also discussed

G. Kalnoor et. al. [4] Said that network security is the most difficult problem to prevent types of malicious attacks and poses a security problem in WSN along with information security application domains. Some of the architectures and guidelines are proposed to protect WSNs (WSN) against various intruder attacks. WSN has a wide range of applications that include mass audiences, the military, etc. The sensors in WSN are implemented in such a way that their detection technology has wireless processing and communication power. The use of traffic analysis to detect anomalies is one of the most efficient and effective techniques for detecting and preventing an intruder. In many WSN applications, a critical issue is protecting the sensor network from adversaries and malicious attacks. Here we discuss some advanced mechanisms of preventive safety and intrusion detection systems that play an important role in the detection and prevention of security attacks in WSN.

S. Bhagat et. al. [5] Said that the WSNs is widespread and that scientists get a lot of enthusiasm for the best applications. The wormhole nodes are false paths that are shorter than the first course in the system that generates problems during the direction of the component, which depend on the reality of the separation between the nodes. The attacking knot traps the plots of true blue knots. In their proposed scrutiny work, they distinguish the wormhole from its powerful node transmission in the system and, moreover, refer the wormhole system to privacy in its modified AODV.

Y. Jiang et. al. [6] Said that service interruption caused by DoS attacks (Denial of Service) is a growing problem in the Internet world and is also a serious problem in the WSNs (WSN). Because of the limited resources and energy of the nodes in the WSN platforms, they have to adapt the security mechanisms according to the characteristics of the WSN. They present an analysis of the five-layer classification of mechanisms available for DoS defense. These defense mechanisms are used to prevent, detect, respond to and tolerate DoS attacks. This document provides a better understanding of the DoS attack problem and allows a security administrator to fight and mitigate the DoS threat

P. Rolla et. al. [7] Proposed a demand sending system dependent on time distribution to distinguish and avoid DoS (Denial of Service) assaults. DoS assaults are overpowering the quantity of access bundles in the system that expend organize control. In the profile-based security conspire (PPS), the conduct of the considerable number of nodes conveyed in the system is watched. At the point when the assailant floods the system with steering demand messages, the aggressor's unusual conduct is in the end recognized. In any case, in the strategy of the Rinvia window, the aggressor is recognized in the way ask for stage and the counteractive action will be done in the course reaction stage. In the proposed system, if any nodes supersede routing demand messages more than dynamic moment, it will be identified as attacker. Also, the node that has distinguished this, will educate others about the ID of the threatening hub. The changed course asks for the conceding stage will proceed until the demand achieves the goal. The goal node won't pick the course containing the identified nodes. Execution is estimated dependent on execution measurements, for example, complete bundle sent, outstanding force, execution, and so forth. In this, the aftereffects of the recreation demonstrate that the proposed work distinguishes and effectively keeps the DoS assault.

S. Hemalatha et. al. [8] Said that, because of the expansion in the application and the requesting highlights, the wireless sensor systems have considered a vital and quickly developing innovation in the segment and, subsequently, get the consideration of the specialists. Concentrating on innovation improvement, energy productivity and viable figuring strategies assume a significant job in deciding the execution of the WSN. Albeit much consideration is paid to the powerful plan of WSN, its qualities that adjust to security issues are imperative in confined circumstances. This archive endeavors to have a successful and productive WSN framework with the security viewpoints got from the antiquated Vedic arithmetic of India. Cross-augmentation conduct of Vedic arithmetic when connected to places where increase of focuses is accessible, a beneficial and enhanced data security is accomplished. Moreover, this work records the execution correlation between Information Security (VMIS) empowered for Vedic Mathematics in WSN with that of Informational Information Security in WSN and has demonstrated that VMIS works superior to the ordinary technique.

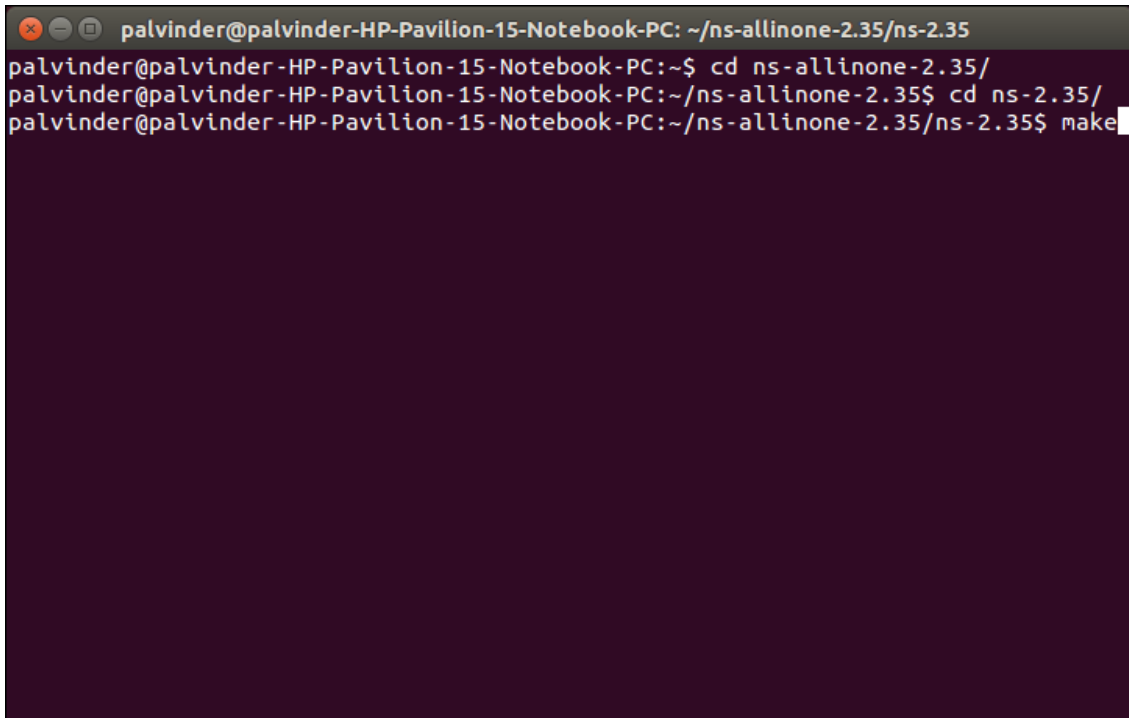
L, Yi et. al. [9] Suggested that the WSNs turns into a rising field of utilization; its security issue has likewise turned into a looked for after objective. This record shows the design and advantages of the WSN application and underscores its security defects. As indicated by different kinds of assaults on wireless sensor arranges, the creator directed a top to bottom investigation and exhibited the WSN security design venture and the comparing explicit methods for barrier.

A. Karakaya et. al. [10] Proposed the WSNs technique that arranges the information acquired by watching the earth handled an expansive number of sensors appropriated in a given zone is sent safely with different sensors or Red focuses. These systems have the capacity not to be associated with a node, to oversee them and not to be associated with a specific red topology, different kinds of a cast, to save the INTEGRITY and the secrecy of the information and the powerful ones. The information acquired from the sensors must be transmitted securely to the objective. RIDES wireless sensors have a ton of sorts of assaults (Sybil, Wormhole, Sinkhole, and so forth.) that undermine the stream of information. When you have a security approach, a general venture must dispense with a few or all assaults. Therefore, arrangements dependent on data security standards have been created, for example, protection, uprightness, accessibility, confirmation and non-disavowal. To the extent information security is concerned, individual information security and the contrary parts of the mystery of genuineness are customized.

3. Implementation Work and Results

There are many techniques which different researchers have proposed in order to attack dos attacks but the major limitation of them is the congestion among those nodes. Due to congestion, the drainage of battery becomes fast and nodes become dead rapidly. So, in this research work, we will distribute the traffic among gateway nodes so as to minimize the traffic load and to enhance the battery depletion problem. Therefore as per the literature survey conducted, the problem is the traffic among every node as every node becomes busy in detection DOS attack.

In the implementation work, firstly we diffused area as 1000*1000 m2, then number of nodes can be taken 50 and traffic type is constant bit rate. Further omni directional antenna type is used. When the simulation is run we have varied number of mobile connectors as 5, 10, 15, 20.



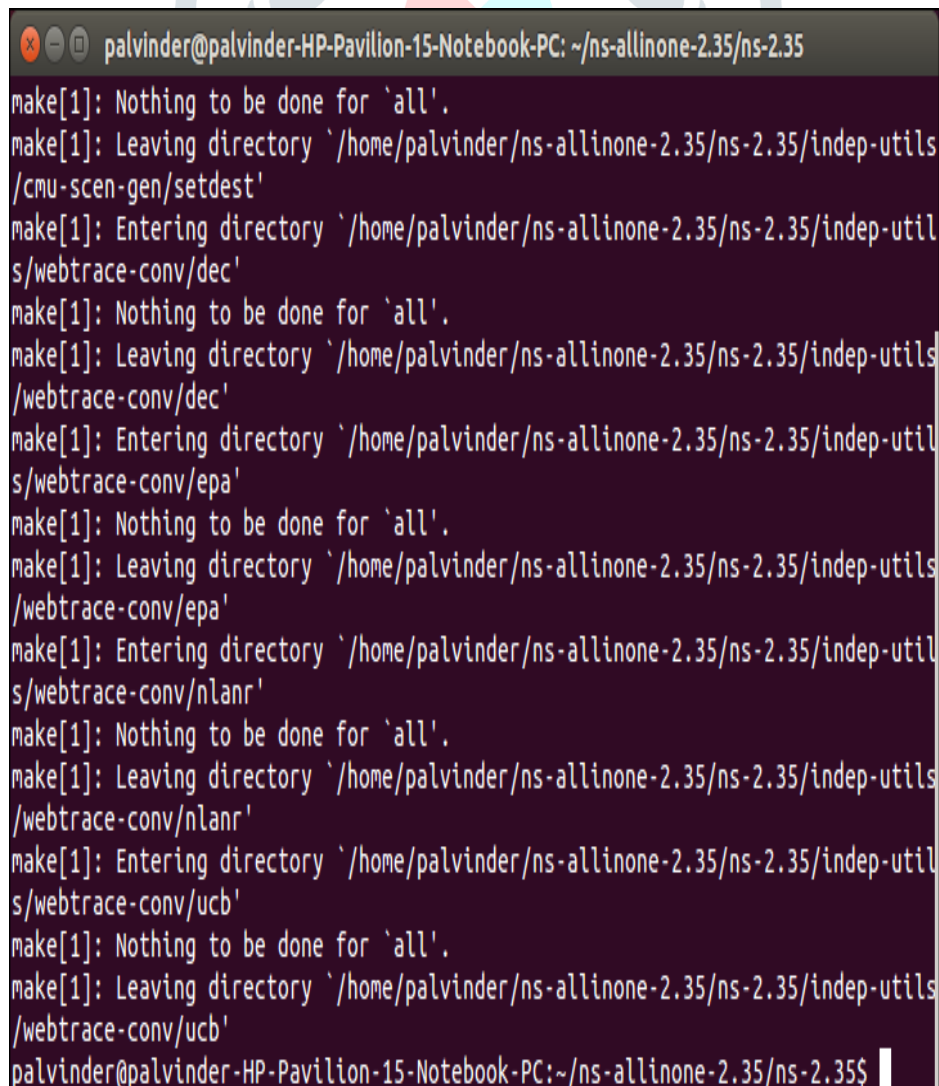
```

palvinder@palvinder-HP-Pavilion-15-Notebook-PC: ~/ns-allinone-2.35/ns-2.35
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~$ cd ns-allinone-2.35/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/ns-allinone-2.35$ cd ns-2.35/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/ns-allinone-2.35/ns-2.35$ make

```

Figure 1. Make Command to Refresh NS2

In the above figure we have used make command to refresh the changes. We have made while doing simulation , this make command is used in the command live as shown in figure above. After this make command , now we are in a position to run our scenario and gathered the results .



```

palvinder@palvinder-HP-Pavilion-15-Notebook-PC: ~/ns-allinone-2.35/ns-2.35
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/cmu-scen-gen/setdest'
make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/dec'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/dec'
make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/epa'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/epa'
make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/nlanr'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/nlanr'
make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/ucb'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/ucb'
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/ns-allinone-2.35/ns-2.35$

```

Figure 2. Scenario with Make Successful

In this figure, the make command success is depicted. After that the ddos.tcl is run as shown below, which is a tcl command. When this tcl command is run, it will first show the number of nodes taken in a scenario. Further simulation is setup and now we are in a position to run our proposed work.

```

palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~$ cd Desktop/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/Desktop$ cd simulation/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/Desktop/simulation$ ns ddos.tcl
num_nodes is set 50
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Loading connection pattern...
Loading scenario file...
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
SORTING LISTS ...DONE!
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44direction for pkt-flow not specified
; Sending pkt up the stack on default.

NS EXITING...
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44i am 44 and dest is 0data dropped by 44i am 44 and dest is 0palvinder@pa
lvinder-HP-Pavilion-15-Notebook-PC:~/Desktop/simulation$ nam ddos_result.nam

```

Figure 3. Simulation Complete

This diagram indicates that the scenario has successfully been completed and NS is exited. Now, we can use name file for looking into the scenario part and look for simulation.

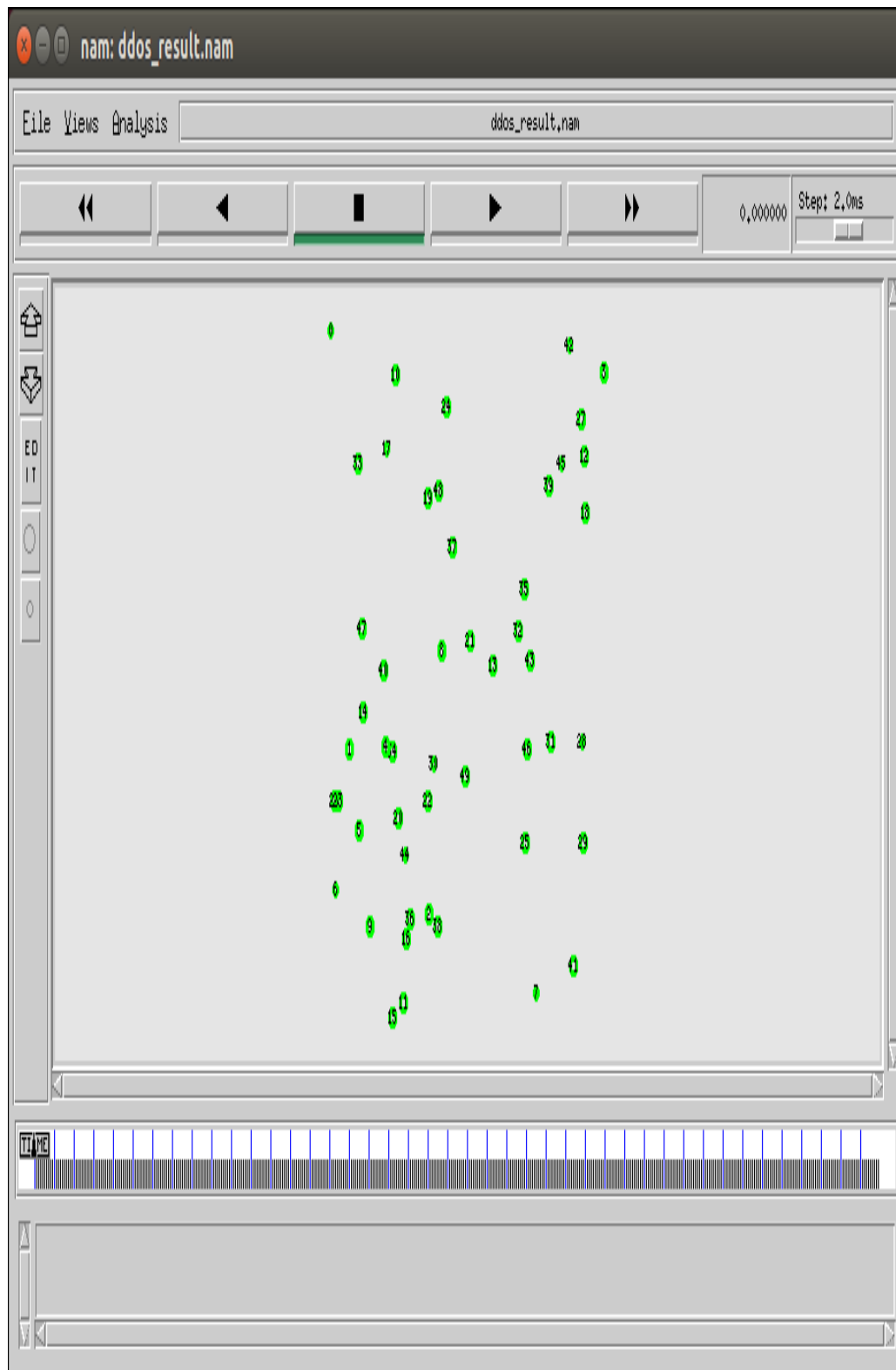


Figure 4. Deployment of various nodes in a network

The above figure shows that the deployment of various nodes in which number of nodes is from 1 to 50. Here the animation file can be run by using play button indicated on the top button and then we can increase the simulation speed using right top scroll button.

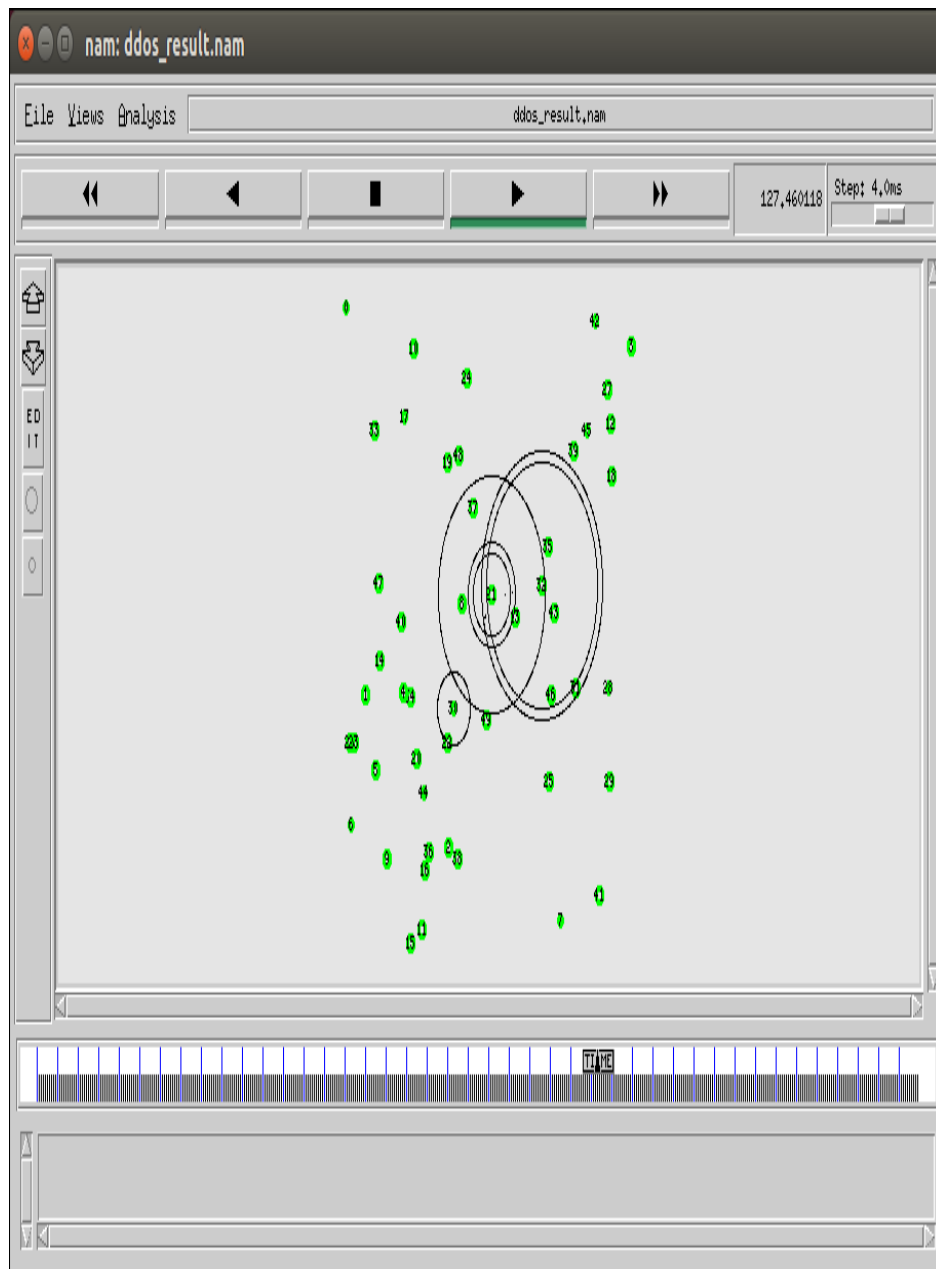


Figure 5. Animation to Show Flooding Attack

This animation diagram indicates the flooding by various nodes in a circle. The flooding is indicated by the number of circles in a nam file as shown in the above diagram.

This next figure represents the command to calculate various parameters

```

palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~$ cd Desktop/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/Desktop$ cd simulation/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/Desktop/simulation$ ns ddos.tcl
num_nodes is set 50
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Loading connection pattern...
Loading scenario file...
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
SORTING LISTS ...DONE!
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44direction for pkt-flow not specified
; Sending pkt up the stack on default.

NS EXITING...
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44i am 44 and dest is 0data dropped by 44i am 44 and dest is 0palvinder@pa
lvinder-HP-Pavilion-15-Notebook-PC:~/Desktop/simulation$ awk -f packetdeliverratio.awk ddos_result.tr

```

Figure 6. Command to calculate various parameters

Results

Performance Metrics

1. Packet Delivery ratio

The package distribution ratio in this simulation is defined as the ratio between the number of packets sent by the constant bit rate sources (CBR, application level) and the number of receiver packets per CBR receives in the destination Table.

Table 1: Packet delivery ratio

No of mobile connections	Base work	Proposed work
5	0.9842	0.9902
10	0.7369	0.8138
15	0.6516	0.6515
20	0.5638	0.8180

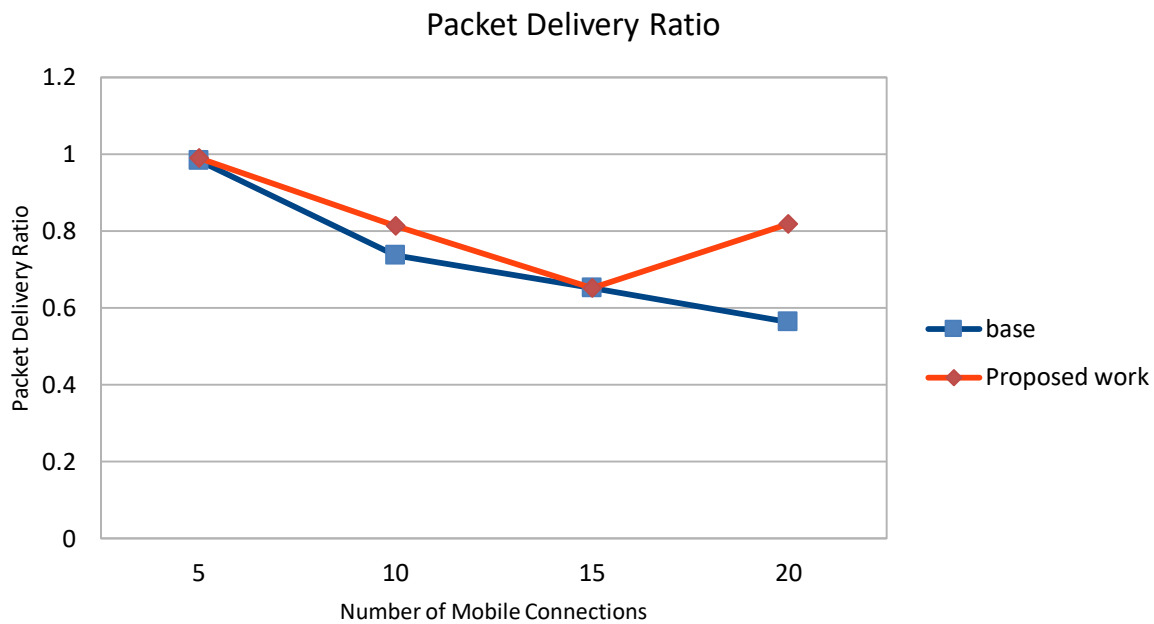


Figure 7. Packet Delivery Ratio

When we set up the number of mobile connections as 5 the packet delivery ratio in case of base work is .9842 while the value in our case appears to be .9902 which is better than our work. Further when the mobile connection is 10 the packet delivery ratio of base work is 0.7369 while value of our work is 0.8138. Again when number of mobile connection is 15 then the packet delivery ratio in base work is 0.6516 and our work value is 0.6515. Again when no of mobile connection is 20 then the packet delivery ratio of base work is 0.5638 but our work value is 0.818. Overall to conclude, our work is better than base work.

2. Throughput: Throughput is total packets success fully delivered to individual destinations in excess of total time.

Table 2. Throughput

No of mobile connection	Base work	New work
5	68.23	68.92
10	141.06	198.39
15	270.24	269.52
20	283.46	183.97

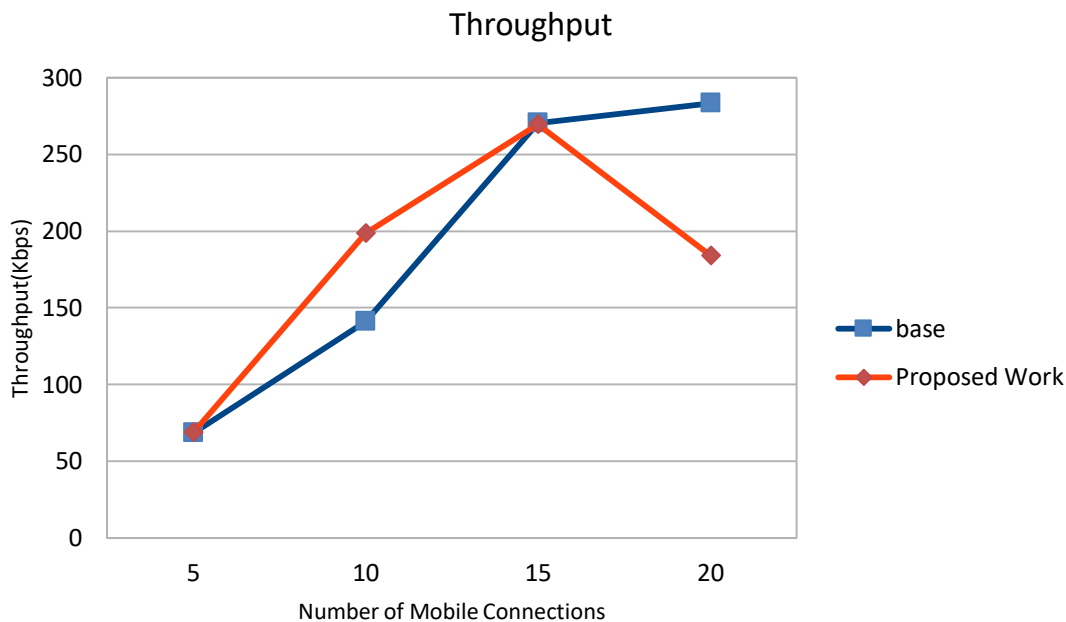


Figure 8. Throughput Analysis

When we set up the number of mobile connections as 5 the Throughput in case of base work is 68.23 while the value in our case appears to be 68.92 which is better than our work. Further when the mobile connection is 10 the Throughput of base work is 141.06 while value of our work is 198.39. Again when number of mobile connection is 15 then the Throughput in base work is 270.24 and our work value is 269.52. Again when no of mobile connection is 20 then the Throughput of base work is 283.46 but our work value is 183.97. Overall trend again suggests that our work is better than base work.

3. Remaining Energy Remaining Energy is defined as the amount of energy left after the simulation is completed successfully.

Table 3. Remaining Energy

No of mobile connection	Base work	New work
5	24.0715	70.0883
10	58.4041	33.8092
15	27.4661	27.2302
20	54.0387	70.0883

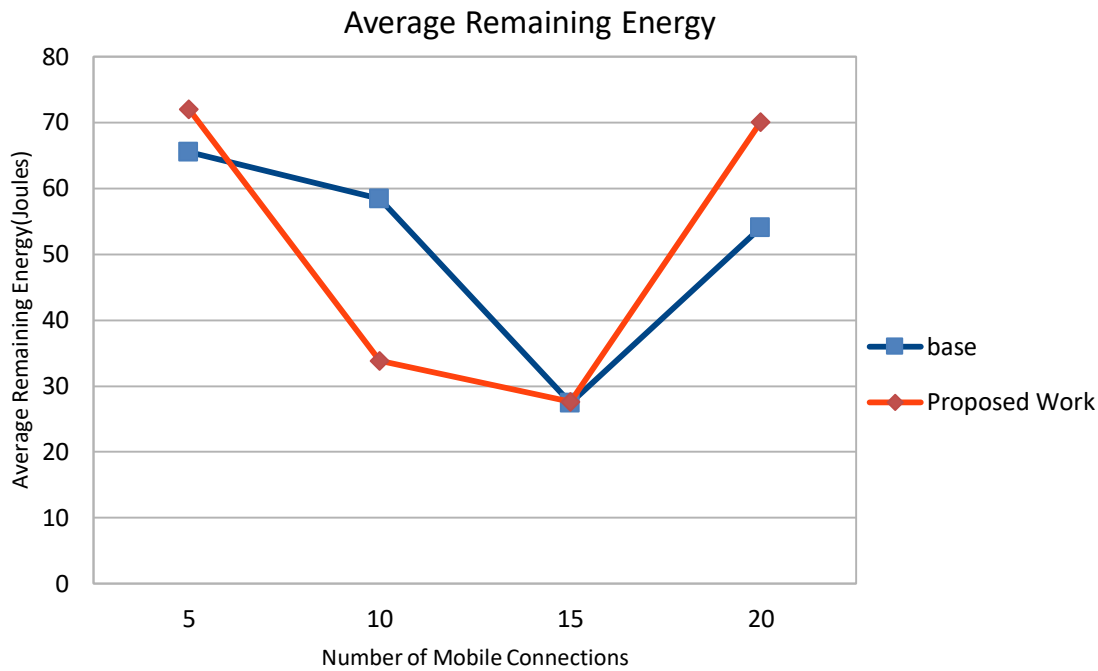


Figure 8. Remaining Energy

When we set up the number of mobile connections as 5 the Remaining Energy in case of base work is 65.5467 while the value in our case appears to be 72.0593 which is better than our work. Further when the mobile connection is 10 the NRL of base work is 58.404 while value of our work is 33.8092 which is less than the base. Again when number of mobile connection is 15 then the NRL in base work is 27.4661 and our work value is 27.2302 which shows the proficiency of proposed work. Again when no of mobile connection is 20 then the NRL of base work is 54.0387 but our work value is 70.0883. Overall trend again suggests it follows the zigzag movement but if we keep on checking the results on different nodes, the remaining energy comes out to be better in the proposed scenario.

4. Delay: Delay is defined as the time the packet takes to reach the destination.

Table 4. Delay

No of mobile connection	Base work	New work
5	41.1214	34.3454
10	105.836	196.863
15	971.766	911.719
20	1074.71	89.3079

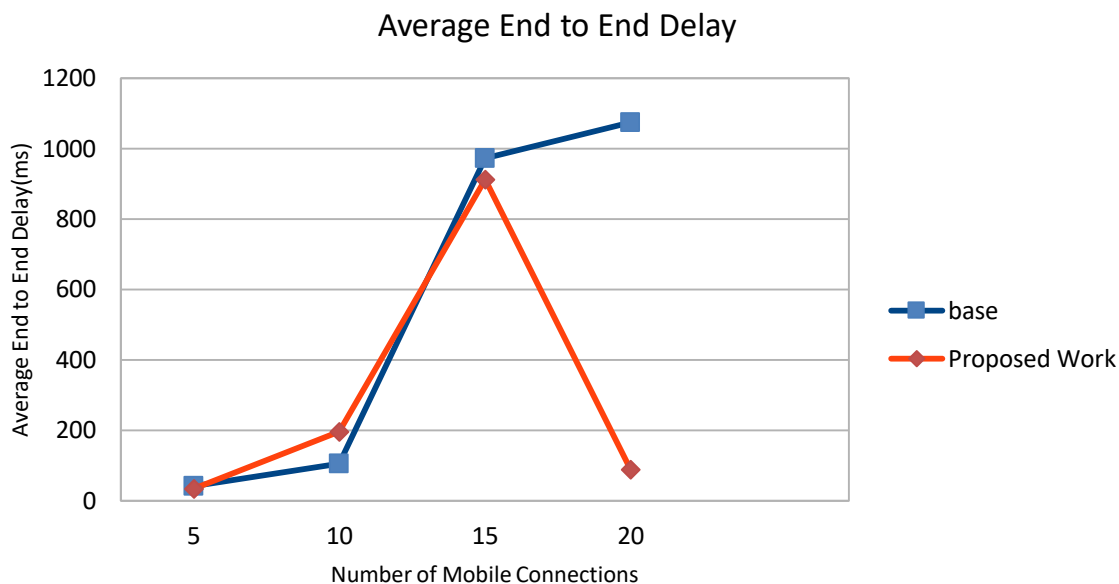


Figure 9. Delay Analysis

When we set up the number of mobile connections as 5 the delay in case of base work is 41.1214 while the value in our case appears to be 34.3453 which is better than base work. Further when the mobile connection is 10 the delay of base work is 105.836 while value of our work is 196.863. Again when number of mobile connection is 15 then the delay in base work is 971.766 and our work value is 911.719. Again when no of mobile connection is 20 then the delay of base work is 1074.71 but our work value is 89.3079. Overall trend again suggests that our work is better than base work.

4. Conclusion

The base work is compared with the proposed approach, which further suggests that proposed approach is better in case of Throughput, Packet Delivery ratio, Remaining Energy and delay. Future Work can be done by taking large network with thousands of nodes because when the network gets large, the complexity gets increases, and hence maintaining such a large list is a difficult task.

References

- [1] P. Dewal ,G.S narula and V. Jain "Detection and Prevention of Black hole attack in clusture based WSNs," IEEE, 2016.
- [2] S. Ali, M. Khan, J. Ahmad, A. Malik and A. Rehman, "Detection and Prevention of Black Hole Attacks in IOT & WSN," Third International Conference on Fog and Mobile Edge Computing (FMEC), 2018.
- [3] R.K Dwivedi, P.Sharma and R.Kumar, "Detection and Prevention Analysis of Wormhole Attack in WSNs," IEEE, 2018.
- [4] G. Kalnoor and J..Agarkhed, "Preventing Attacks and Detecting Intruder for Secured WSNs," IEEE, 2016.
- [5] S. Bhagat and T. Panse, "A Detection and Prevention of Wormhole Attack in homogeneous WSNs," IEEE, 2016.
- [6] Y. Jiang, J. Huang and W. Jin, "Intrusion tolerance system against denial of service attacks in WSNs " The 28th Research Institute of CETC, Nanjing, China, 2014.
- [7] P. Rolla and M. kaur, "Dynamic Forwarding Window Technique against DoS Attack in WSN," International Conference on Micro-Electronics and Telecommunication Engineering, 2016.
- [8] S.Hemalatha and V.Rajamani, "VMIS: An Improved security mechanism for WSN applications" 1st International Conference on Science, Engineering and Management Research, Chennai, India, IEEE, 2014.
- [9] L.Yi and F. Zhongyong, "The Research of Security Threat and Corresponding Defense Strategy for WSN," Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015.
- [10] A. Karakaya and S. Akleyek, "A Survey on Security Threats and Authentication Approaches in WSNs," IEEE, 2018.